ANALYSIS

29(114), March 1, 2015

ISSN 2278–5469 EISSN 2278–5450

Discovery

A Survey on software integrity attestation solutions for multi tenant cloud systems

Thomas Gowtham J[1], Arun Kumar K[2]

1.PG Scholar, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore-641035, Tamil Nadu, India; E-mail: jgowtham1990@gmail.com

2.Assistant Professor, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore-641035, Tamil Nadu, India; E-mail: arunkumarbite@gmail.com

Publication History

Received: 11 January 2015

Accepted: 17 February 2015

Published: 1 March 2015

Citation

Thomas Gowtham J, Arun Kumar K. A Survey on Software Integrity Attestation Solutions for Multi Tenant Cloud Systems. *Discovery*, 2015, 29(114), 164-167

ABSTRACT

Cloud systems present a cost-effective service hosting infrastructure for application service providers (ASPs). Cloud systems are often shared by multiple tenants from a variety of security domains, which make them susceptible to various malicious attacks. Furthermore, cloud systems habitually host long running applications such as substantial data processing. This provides opportunities for attackers to take advantage of the system vulnerability and perform tactical attacks. There are several software integrity attestations solutions for this problem. This article focuses on those software integrity attestation solutions.

Keywords: Integrity Attestation, cloud computing

1. INTRODUCTION

Cloud computing is the deliverance of computing as a service rather than a product, hereby shared resources and software are provided to computers and other devices as utility (like the electricity grid) over a network (typically the Internet). Cloud computing has become known as a capable hosting platform that let several cloud users called tenants to share a common physical computing infrastructure. With speedy acceptance of the concepts of Software as a Service (SaaS) and Service Oriented Architecture (SOA), the Internet has evolved into an important service delivery infrastructure instead of only providing host connectivity. The problem is attackers can act as if he/she is a legitimate service provider to provide fake service components, and the service components provided by benevolent service providers may include security holes that can be demoralized by attackers. In large-scale multitenant cloud systems, several malicious attackers may instigate colluding attacks on certain targeted service functions to nullify the assumption.

2. RELATED WORK

A. Run Test

RunTest is a scalable runtime integrity attestation framework to guarantee the integrity of dataflow processing in cloud infrastructures. It provides light-weight application level attestation methods to dynamically authenticate the integrity of data processing results and identify malicious service providers when inconsistent results are detected. It is a light weight application level attestation scheme that can dynamically confirm the integrity of data processing outcome in the cloud infrastructure and discover malicious service providers when inconsistent results are spotted. It validates service integrity by combining and analyzing result consistency information more willingly than evaluating memory footprints of code execution as used by code attestation. This approach does not need trusted hardware or secure kernel co-subsisted with intermediary service providers in the cloud. The foundation behind this approach is that dataflow processing applications are mostly apprehensive about the accuracy of final data results instead of the integrity of the code execution. Unlike customary agreement-based Byzantine fault detection schemes, this approach does not rely on full time majority voting on all service nodes, which falls short for cloud infrastructures in terms of scalability. This work makes the first effort to offer efficient runtime integrity attestation method for dataflow processing in the cloud infrastructure.

Run Test makes the following contribution:

- It provides a new runtime service integrity attestation method that employs a novel attestation graph model to capture attestation results amongst different cloud nodes. The design is a clique based attestation graph analysis algorithm to identify malicious service providers and recognize colluding attack models. Our scheme can attain runtime integrity confirmation for cloud dataflow processing services using a small number of attestation data.
- The RunTest is implemented within IBM System dataflow processing system and tested it on NCSU virtual computing lab (VCL), a production virtual cloud infrastructure. The prototype implementation indicates that our scheme can be effortlessly integrated into cloud dataflow processing system.

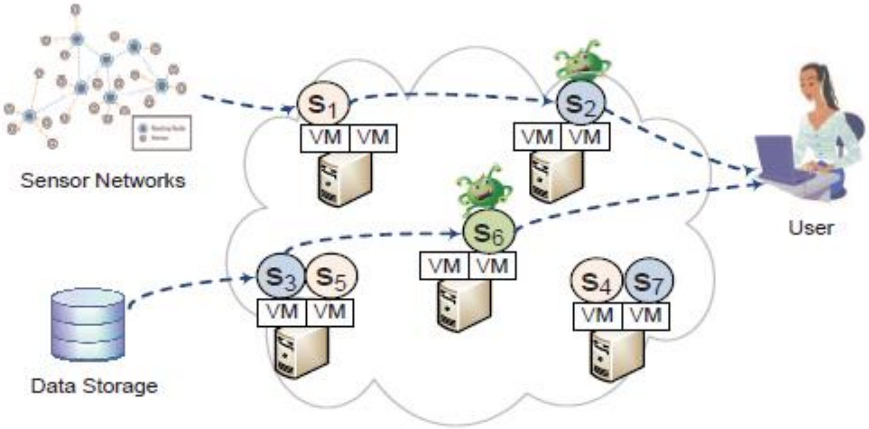

Figure 1 Integrity attack in cloud-based data processing

B. AdapTest:

AdapTest is a novel adaptive runtime service integrity attestation framework for large scale cloud systems. AdapTest builds on top of our previously developed system RunTest that performs randomized probabilistic attestation and employs a clique-based algorithm to identify malicious nodes. However, randomized attestation still imposes significant overhead for high throughput multi-hop data processing services.

In contrast, AdapTest dynamically verifies the trustiness of different services based on previous attestation results and adaptively selects attested services during attestation. Thus, AdapTest can considerably decrease the attestation overhead and cut down the detection delay.

AdapTest makes the following offerings:

- This model provides a new adaptive multi-hop integrity attestation framework based on a new weighted attestation graph model. We obtain both per-node trust scores and pair-wise trust scores to efficiently guide probabilistic attestation.
- AdapTest is implemented on the IBM System S stream processing system and tested it on the virtual computing lab (VCL), a production virtualized computing cluster that operates in a similar way as Amazon EC2. Our experimental results show that AdapTest can considerably decrease attestation overhead for reaching the 100% detection rate by up to 60% and cut down detection time by up to 40% compared to previous randomized attestation approaches.

C. *IntTest*

IntTest provides a novel integrated attestation graph analysis scheme that can provide stronger attacker pinpointing power than previous schemes. Moreover, IntTest can automatically enhance result quality by replacing bad results produced by malicious attackers with good results produced by benign service providers. IntTest can not only pinpoint attackers more efficiently but also can suppress aggressive attackers and limit the scope of the damage caused by colluding attacks. Moreover, IntTest provides result auto correction that can automatically replace corrupted data processing results produced by malicious attackers with good results produced by benign service providers.

3. ATTACK MODEL

In a shared cloud infrastructure, malicious attackers can pretend to be legitimate service providers to give fake service instances or compromise vulnerable benign service instances by exploiting their security roles. It focuses on detecting the service integrity attack where a malicious (or compromised) service instance gives deceptive data processing results.

To escape detection, malicious attackers may want to perform selective cheating. That is, they can misbehave on a selective subset of received data while pretending to be benign on other received data. Thus, the attack detection scheme must be able to capture misbehavior that are both unpredictable and occasional without losing scalability. Although we can perform integrity attestation on all service instances all the time, the overhead of integrity attestation would be very high, especially for high throughput data processing services in large-scale cloud systems. Thus, an effective attack detection scheme must perform sneaky attestation, which can prevent attackers from gaining knowledge about our attestation scheme (i.e., when and which set of data will be attested). Otherwise, the attacker can compromise the integrity of selective data processing results without being detected at all.

Furthermore, cloud computing infrastructures often comprise a large number of hosts running many more VMs and application service instances. It creates new opportunities for colluding attacks where multiple malicious attackers launch coordinated attacks or multiple benign service instances are simultaneously compromised and controlled by a single malicious attacker. Colluders can communicate with each other in an arbitrary way and produce the same incorrect results on the same input. Attackers can also change their attacking and colluding strategies arbitrarily. However, we assume that attackers do not have knowledge of other benign service instances that they do not interact with.

4. COMPARATIVE ANALYSIS OF THE ABOVE TECHNIQUES

Algorithm/Parameters	Detection			Attestation overhead	False alarm rate
	rate	delay	time		
Runtest	Low than IntTest	More delay than IntTest, AdapTest	Higher than AdapTest	More than AdapTest	NA
AdapTest	NA	NA	40% lesser than RunTest	60% lesser than RunTest	NA

IntTest	High than Runtest but not 100 %	NA	Less than runtest	Same as AdapTest	Lower than all

5. CONCLUSION

Amongst the three software integrity attestation techniques for multi tenant cloud system, IntTest is the recent solution for the problem. Although both RunTest and AdpaTest have certain advantages, IntTest overcomes the limitations of the two previous approaches. The IntTest is evaluated with an additional metric of false alarm rate hence providing more accurate results than the previous approaches.

REFERENCE

1. J. Du, W. Wei, X. Gu, and T. Yu, “Runtest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2010.
2. J. Du, N. Shah, and X. Gu, “Adaptive Data-Driven Service Integrity Attestation for Multi-Tenant Cloud Systems,” Proc. Int’l Workshop Quality of Service (IWQoS), 2011
3. J. Du, D. J. Dean, Y. Tan, X. Gu, Ting Yu, “Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds” IEEE transactions on parallel and distributed systems, vol. 25, no. 3, march 2014
4. Software as a Service, http://en.wikipedia.org/wiki/Software as a Service, 2014